Zero-Knowledge Proof Systems and their Application to Privacy Protection

Dieter Sommer[1] <dso@zurich.ibm.com>

The talk first presents the well-established notion of zero-knowledge proof systems [1]. A zero-knowledge proof system allows a prover to proof an assertion to a verifier without revealing any other information than the correctness of the assertion. The proof system of Schnorr [2] for proving that one knows the discrete logarithm of a mutually known group element without actually revealing the logarithm is presented and a proof sketch of the correctness is given.
We sketch the application of proof systems for proving knowledge of discrete logarithms to anonymous credential systems [3]. A credential in this context is a certificate, i.e., a signature on a list of attributes, that can, unlike classical certificates, be used to prove properties about its attributes and to proof that one has (knows) a signature on the attributes without actually revealing the credential. Proof protocol instances involving a particular credential are mutually unlinkable and unlinkable to the issuance of the credential. An example application of such anonymous credential systems is authorization on the Internet.
The talk is targeted at a general mathematical audience and does not require background in cryptography.

[1] Shafi Goldwasser, Silvio Micali and Charles Rackoff: *The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract)*, STOC 1985, pp. 291–304
[2] Claus Peter Schnorr: *Efficient signature generation for smart cards*, Journal of Cryptology, vol. 4, no. 3, pp. 161–174 (1991)
[3] Jan Camenisch and Anna Lysyanskaya: *An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation*, EUROCRYPT 2001, pp. 93–118

[1]IBM Research